UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR HISTORICAL CELL SITE INFORMATION	MAGISTRATE NO. H-10-998M MAGISTRATE NO. H-10-990M MAGISTRATE NO. H-10-981M

AMICI ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND ACLU OF TEXAS' BRIEF IN OPPOSITION TO THE GOVERNMENT'S REQUEST FOR REVIEW

The Electronic Frontier Foundation, American Civil Liberties Union ("ACLU") and ACLU of Texas respectfully submit this brief in opposition to the government's request for review.[1] This case addresses the standard the government must meet to obtain historical cell site location information ("CSLI"). The resolution of this question will have a significant impact on the privacy of the hundreds of millions of Americans who carry a cell phone.[2] Given the invasive nature of cell phone tracking, we urge the Court to uphold the magistrate judge's decision to deny the government's application and require the government to obtain a warrant and show probable cause prior to tracking cell phones.

As described in greater detail below, the Stored Communications Act grants courts the discretion to deny an application for a court order under 18 U.S.C. § 2703(d) and instead require a search warrant based on probable cause. Considering the doctrine of constitutional avoidance, it is particularly appropriate for a court to use that discretion when faced with an application that raises serious constitutional questions, and such questions are clearly posed by the government's attempt to obtain CSLI without probable cause. The Supreme Court's case law on tracking devices and persuasive circuit authority makes clear that cell phone tracking permits the

[1] The interests of all three organizations in this litigation is described in their motions for leave to file amicus briefs. Doc. Nos. 10, 14.
[2] CTIA, *CTIA's Semi-Annual Wireless Industry Survey*, *available at* http://files.ctia.org/pdf/CTIA__Survey_Midyear_2010_Graphics.pdf (last viewed Dec. 13, 2010).

government to engage in the sort of prolonged surveillance encompassing protected spaces that the Fourth Amendment only permits with a valid warrant based on probable cause. The government's reliance on the Court's jurisprudence regarding bank records and dialed telephone numbers is misplaced, because CSLI is not voluntarily communicated to mobile providers in the same way that banking transactions and dialed numbers are disclosed. Further, the government's fallback argument that it should only have to demonstrate that its request is reasonable even if the Fourth Amendment applies carries little weight because the case law it draws on, addressing subpoenas, invariably involves notice to the person whose records are at issue.

Additionally, although the government objects to the magistrate judge's factual conclusions, the Federal Rules of Evidence do not apply to courts' consideration of government applications for § 2703(d) orders and the judge relied on valid facts in reaching his conclusion. The government's late-filed affidavit does not call these facts into question but, if the Court disagrees, the appropriate course of action is to remand to the magistrate judge for further consideration.

I. The Stored Communications Act Grants Courts the Discretion to Deny Government Applications for Orders Under 18 U.S.C. § 2703(d).

Although the Stored Communications Act ("SCA") allows the government to obtain historical cell site location information ("CSLI") using a court order issued under 18 U.S.C. § 2703(d), the statute also provides magistrates the discretion to deny applications for such orders even when the government has made the factual showing required under that section. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 315-17 (3d Cir. 2010) (hereinafter "*Third Circuit Opinion*"), *pet. for reh'g en banc denied* (3d Cir. Dec. 15, 2010). As the Third Circuit has explained, the statute does so by its use of the phrase "only if" in § 2703(d), indicating that the "specific and articulable facts" showing required by that section is a necessary but not necessarily sufficient condition for the issuance of a § 2703(d) order. *Id.* The practical effect of such a denial is that the government must instead proceed by obtaining a search warrant based on probable cause,

issued under Rule 41 of the Federal Rules of Criminal Procedure pursuant to 18 U.S.C. § 2703(c)(1)(a). *See id.* at 316. Therefore, "the statute as presently written gives the [magistrate judge] the option to require a warrant showing probable cause. . . ." *Id.* at 319.[3]

The intent of this "sliding scale" construction of § 2703 is evidenced by Congress' recognition that the Fourth Amendment may in some cases protect the privacy of information that would otherwise be available to the government under § 2703(d). As the Senate Judiciary Committee's report on the statute explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information *may* be subject to no constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986) (emphasis added); *see also, e.g.*, S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are *not always clear or obvious*.") (emphasis added). In the context of such Fourth Amendment uncertainty, it makes sense that Congress would provide a constitutional safety-valve for judges considering government applications under § 2703(d), future-proofing the statute by allowing

[3] Amici's prior briefs to the Third Circuit and the Western District of Pennsylvania provide extensive support for the *Third Circuit Opinion*'s holdings. *See* Brief for Electronic Frontier Foundation, American Civil Liberties Union, ACLU Foundation of Pennsylvania, and Center for Democracy and Technology as Amici Curiae Opposing the Government's Request for Review, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, Magistrate's No. 07-524M, 2008 WL 4191511 (W.D. Pa. 2008), *available at* https://www.eff.org/files/filenode/celltracking/LenihanAmicus.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Affirmance, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/filenode/celltracking/Filed%20Cell%20Tracking%20Brief.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Opposing Rehearing En Banc, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/Filed_Amicus_Opp_to_En_Banc_Petition.pdf

courts the discretion to deny such applications in order to avoid potential constitutional violations or unnecessary constitutional rulings.

This plain language reading of the statute, allowing courts to avoid such serious constitutional questions by giving judges the discretion to require warrants, is not only consistent with but is required by the doctrine of constitutional avoidance. The constitutional avoidance doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 78 (1994); *see also Clark*, 543 U.S. at 384 (courts must adopt any "plausible" construction that would avoid a serious constitutional concern).

The statute places no restrictions on the discretion it grants to magistrates, *see Third Circuit Opinion*, 620 F.3d at 319, but of course that discretion is not boundless: "[N]o judge in the federal courts has *arbitrary* discretion . . . ." *Id*. at 316 (emphasis added). Rather, a magistrate's decision to require a warrant "must be supported by reasons" justifying a divergence from § 2703(d)'s specific and articulable facts standard. *Id*. at 316-17. In other words, courts clearly may not *abuse* the discretion that has been granted to them. As the Supreme Court has explained, "[d]iscretion is not whim…." *Martin v. Franklin Capital Corp.*, 546 U.S. 132, 139 (2005). A court must have reasons to support its use of discretion. A court abuses its discretion when "it base[s] its ruling on an erroneous view of the law or on a clearly erroneous assessment of the evidence." *Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384, 405 (1990).

In light of the discretion granted to courts by Congress in § 2703(d), and particularly in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies, it is clear that when faced with a government application that raises a serious constitutional question the appropriate course for a magistrate is to avoid that question by exercising its discretion and denying that application. *See City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) ("The judiciary risks error by elaborating too

fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").[4] It is equally clear under the doctrine of constitutional avoidance that this court need not endeavor to definitively answer the serious Fourth Amendment question posed by the government's application in order to affirm the magistrate's denial, but instead need only recognize that it *does* raise a serious Fourth Amendment question.

As amply demonstrated by the magistrate judge's comprehensive opinion, and as fully explained below, such a question is obviously present in this case. However, to the extent this Court disagrees with the Third Circuit and finds no room for discretion in § 2703(d), the answer to this serious Fourth Amendment question is clear: cell phone users do have a reasonable expectation of privacy in their location, and the government must obtain a warrant before acquiring CSLI from a cell phone provider.

II. The Magistrate Judge's Denial of the Government's Application Was Not an Abuse of Discretion.

This Court should uphold the magistrate judge's decision to deny the government's application and instead require the government to obtain a warrant and demonstrate probable cause. That decision was both correct as a matter of fact and law, and a proper use of the magistrate judge's discretion under 18 U.S.C. § 2703(d). As explained below, the magistrate judge's factual findings were not clearly erroneous but rather permissible and proper, and the government's objection that the magistrate judge did not satisfy Federal Rule of Evidence 201 is a red herring because the Federal Rules of Evidence are not applicable to courts' consideration of

[4] Importantly, the panel majority in the *Third Circuit Opinion* did not hold that the magistrate must conclude that the Fourth Amendment definitely would be violated by issuance of a § 2703(d) order before she may exercise her discretion to deny the application, as the concurring panelist recognized. *Third Circuit Opinion* at 319-320 (Tashima, J., concurring). Rather, the panel plainly expected the magistrate to determine whether the requested order *may* violate the Fourth Amendment. Read in this manner, the import of the panel majority's final directive to the magistrate in that case—that any conclusion that a warrant is "required" be supported by factual findings and a full explanation, *id*. at 319—becomes clear. To the extent the magistrate were to conclude that government acquisition of CSLI absent probable cause may possibly violate the Fourth Amendment, it would indeed be "required" by the doctrine of constitutional avoidance to use the constitutional safety valve provided by Congress and avoid that serious Fourth Amendment question by requiring a warrant.

government applications for court orders under 18 U.S.C. § 2703(d). Moreover, the magistrate judge was correct to conclude based on Supreme Court and persuasive circuit court precedent that cell phone users possess a reasonable expectation of privacy in CSLI, that the expectation of privacy in CSLI is not eliminated by analogy to bank records or dialed telephone number information, and that the government must obtain a search warrant based on probable cause before obtaining such private records.

A. The Magistrate Judge's Factual Findings Were Permissible and Proper.

The government objects to the court's "improper use of judicial notice." Gov. Br. at 5. It argues both that the court failed to provide it with adequate notice of the facts upon which the court intended to rely, Gov. Br. at 6-7, and that the facts at issue were not appropriate for judicial notice, Gov. Br. at 7-10. The government's focus on judicial notice is misplaced. The court's factual findings were permissible, but its reliance on Federal Rule of Evidence 201 was unnecessary. The Federal Rules of Evidence do not apply to hearings on whether to grant or deny applications for § 2703(d) orders, so there was no need for the court to comply with Federal Rule of Evidence 201. Furthermore, as the Third Circuit concluded, magistrate judges have the discretion to require the government to show probable cause. *Third Circuit Opinion*, 620 F.3d at 319. Because the district court's factual findings were not clearly erroneous, they should be permitted to stand. If the court believes the government's late-filed declaration from MetroPCS calls those findings into doubt, the proper course is to remand for a fuller evidentiary hearing.

1. The Federal Rules of Evidence Do Not Apply.

Federal Rule of Evidence 1101 addresses when the evidence rules apply. Subpart (d) provides a list of instances in which the evidence rules are inapplicable. It states:

> The rules (other than with respect to privileges) do not apply in the following situations:
>
> (1) Preliminary questions of fact. The determination of questions of fact preliminary to admissibility of evidence when the issue is to be determined by the court under rule 104.
>
> (2) Grand jury. Proceedings before grand juries.

> (3) Miscellaneous proceedings. Proceedings for extradition or rendition; preliminary examinations in criminal cases; sentencing, or granting or revoking probation; issuance of warrants for arrest, criminal summonses, and *search warrants*; and proceedings with respect to release on bail or otherwise.

Fed. R. Evid. 1101(d) (emphasis added). The list does not include applications for § 2703(d) orders. However, that does not mean the rules apply to adjudications of these applications. A variety of courts and a leading treatise have concluded that the list is illustrative rather than exclusive. 31 Charles Alan Wright and Victor James Gold, Federal Practice and Procedure § 8075 (1st ed. 2010); *United States v. Frazier*, 26 F.3d 110, 113 (11th Cir. 1994) (the "absence of supervised release" from Rule 1101(d) "does not change our conclusion that the Federal Rules of Evidence do not apply to supervised release revocation proceedings."); *United States v. Singer*, 345 F. Supp. 2d 230, 234 (D. Conn. 2004) ("Rule 1101(d)(3) has never been read as giving an exhaustive list of proceedings exempted from the application of the Federal Rules of Evidence."); *United States v. Weed*, 184 F. Supp. 2d 1166, 1173 (N.D. Okla. 2002) ("[T]he Court agrees that Rule 1101(d)(3) does not provide an exhaustive list of exceptions"); *United States v. Zannino*, No. 83-235-N, 1985 WL 2305, at *3 (D. Mass. June 5, 1985) (Rule 1101(d)(3) exceptions not "an exclusive and exhaustive list.").

Amici can find no cases squarely addressing whether the Federal Rules of Evidence apply when courts consider § 2703(d) orders. However, there are good reasons to conclude that the evidence rules are inapplicable. Search warrants are expressly exempt from Federal Rule of Evidence 1101(d)(3) because, as the advisory committee explained, the "nature of the proceedings makes application of the formal rules of evidence inappropriate and impracticable." Fed. R. Evid. 1101, Advisory Committee's Note to Subdivision (d). The same holds true for § 2703(d) applications. These applications are often time-sensitive, and it would neither be practical nor in some cases even possible for the government to comply with the evidence rules. For example, the prohibition on hearsay would mean that agents would not be able to recite in affidavits the information provided to them by confidential informants. Rather, the informants themselves would have to provide testimony, which would itself be limited by the hearsay rule. Applying the evidence rules to § 2703(d) applications would invalidate the governments'

longstanding practice, heretofore unquestioned by courts, of relying on hearsay-laden affidavits of law enforcement agents as a basis for applications to obtain cell site information. *See, e.g., In re Application of U.S. for an Order: (1) Authorizing Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing Disclosure of Location-Based Services*, 727 F. Supp. 2d 571 (W.D. Tex. 2010) (affidavit accompanied cell site application); *In re Application of U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number ESN Cell Phone Number ESN Cell Phone Number ESN*, Misc. No. 06-0186, 187, 188, 2006 WL 6217584 (D.D.C. Aug. 25, 2006) (same).

In *Frazier*, the Eleventh Circuit held that even though hearings on supervised release were not specifically mentioned in Federal Rule of Evidence 1101(d), they are sufficiently similar to probation and parole hearings which Rule 1101(d) exempts that it was appropriate to exempt supervised release hearings as well. *Frazier*, 26 F.3d at 113. In a similar vein, this Court should analogize between search warrants and § 2703(d) applications and conclude that the evidence rules do not apply to adjudications of either one.

Federal Rule of Evidence 201 does not apply for the simple reason that the Federal Rules of Evidence do not apply to adjudications of government applications to obtain § 2703(d) orders.

2. The Magistrate Judge's Factual Determinations Were Proper.

The court's factual determinations were proper. As discussed previously, courts have the discretion to require the government to obtain a warrant and demonstrate probable cause to access CSLI. *Third Circuit Opinion*, 620 F.3d at 319. Courts are not permitted to abuse their discretion, therefore the question this court should ask is whether the court below "based its ruling on . . . a clearly erroneous assessment of the evidence." *Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384, 405 (1990). The court did not do so. As the court below noted, its "most significant findings" were based on expert testimony given to Congress. *Smith Op.*, 2010 WL 4286365, at *2. This testimony is reliable evidence. It was offered by Matt Blaze, who is a Professor at the University of Pennsylvania. He has a Ph.D. in Computer Science from Princeton

University, 12 years of industry experience, and his academic focus is "the properties and capabilities of surveillance technology." *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1-2 (2010) (statement of Professor Matt Blaze), *available at* http://www.crypto.com/papers/blaze-judiciary-20100624.pdf. His testimony squarely addresses the technology at issue, and the government says nothing that calls into question Professor Blaze's credentials or the veracity of his testimony.

The government's initial application remains sealed, so amici are uncertain what facts the government submitted to the magistrate judge prior to his decision. The government's decision to obtain a declaration from MetroPCS after the decision suggests that it did not offer evidence regarding the technical aspects of cell phone tracking that the magistrate judge and many other courts around the country have considered essential to determining whether tracking is lawful. When viewed in this light, the magistrate judge's decision to utilize Congressional testimony offered by a well-credentialed expert is all the more reasonable.

It is properly the government's burden to show that its application is lawful. *Accord United States v. Coreas*, 419 F.3d 151, 158 (2d Cir. 2005) ("[I]t is the Government's burden to provide probable cause to believe that a defendant was undertaking some unlawful activity before a search warrant may issue."). If anything hinges on the precision of the tracking, then the government's failure to proffer facts regarding precision means it has failed to meet that burden.

If this Court determines that the MetroPCS affidavit—which the magistrate judge never had the opportunity to see—calls the magistrate judge's factual findings into question, then it should remand for further consideration in light of the new information. In the Third Circuit case, for example, the panel majority, mindful of the limits on discretion, concluded that the magistrate judge had exceeded them by reaching a legal conclusion not supported by the factual record. In particular, the panel majority held that the magistrate's legal conclusion that cell site location information (CSLI) is protected by the Fourth Amendment was based on a factual

premise that the sparse factual record did not support, *i.e.*, the premise that CSLI by definition is precise enough to reveal information about the interior of Fourth Amendment-protected spaces such as the home. *See Third Circuit Opinion*, 620 F.3d at 312-13 (considering whether there was "any basis" for the magistrate's holding and concluding that "there [was] no evidence in this record" that CSLI was so revealing); *see also id. at 317* (faulting the magistrate for "declin[ing] to issue a § 2703(d) order on legal grounds without developing a factual record"). In other words, the panel concluded that by "bas[ing] its ruling on . . . a clearly erroneous assessment of the evidence," *Bowers v. Nat'l Collegiate Athletic Ass'n*, 475 F.3d 524, 538 (3d. Cir. 2007) (internal quotation marks and citation omitted), the magistrate court had abused its discretion. It therefore remanded to the magistrate with a caution that any further exercise of discretion must be supported by factual findings and a "full explanation" of the court's reasoning. *Third Circuit Opinion*, 620 F.3d at 319. To the extent that this Court finds that the magistrate judge's factual findings were improper, then the way forward is for this court to remand, as the Third Circuit did.

B. Warrantless Government Access to CSLI Raises a Serious Fourth Amendment Question Justifying the Magistrate Judge's Exercise of His Discretion Under 18 U.S.C. § 2703(d).

1. Cell Phone Users Have a Fourth Amendment-Protected Reasonable Expectation of Privacy in CSLI.

The magistrate judge, far from abusing his discretion under § 2703(d), properly relied on Supreme Court and persuasive Circuit Court precedent to conclude that cell phone users have a Fourth Amendment-protected reasonable expectation of privacy in CSLI. Based on the Supreme Court's holding in *United States v. Karo*, 468 U.S. 705 (1984), and following the lead of the *Third Circuit Opinion* and *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), *pet. for reh'g en banc denied* (D.C. Cir. Nov. 19, 2010), the magistrate here correctly concluded that CSLI is protected by the Fourth Amendment because individuals have a reasonable expectation of privacy in their location and movement information, which can reveal intimate details of their lives—not only their presence in protected locations like their home or office, but their doctors'

visits, shopping habits, attendance at church, or association with others.

Over a quarter of a century years ago, the Supreme Court in *Karo* held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device known as a beeper inside a can of ether and used it to infer that the ether remained inside a private residence. 468 U.S. at 708-10. In considering the Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id*. at 714-15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, *id*. at 707, whether it reveals that information directly or enables inferences about the contents of protected spaces. *See also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

Therefore, and as the magistrate judge correctly held, *Karo* and *Kyllo* compel the conclusion that CSLI implicates Fourth Amendment interests because it directly reveals or enables the government to infer information about whether the cell phone is inside a protected location and whether it remains there. The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals' reasonable expectations of privacy. *See, e.g. Kyllo*, 533 U.S. at 31 (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486 (1964) (hotel room). This is true even if CSLI is as imprecise as the government claims,[5]

[5] The affidavit does not establish the precision with which an individual could be tracked via the MetroPCS network. The affidavit states that the radius of its towers range from 100 yards to five

because as the magistrate judge noted, even imprecise information when combined with visual surveillance or a known address can enable law enforcement to infer the exact location of a phone. *Smith Op.* at *7, n. 69. Indeed, that is exactly how the government's experts routinely use such data; as the *Third Circuit Opinion* notes, "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home." *Third Circuit Opinion* at 311-12.

However, even if this Court is not prepared to conclude on the present factual record that CSLI is protected under *Karo* and *Kyllo* as the magistrate did, there is at least enough information in the present record for this Court to conclude, as a majority of the *Third Circuit Opinion* panel concluded, that it "cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject" and is therefore protected under *Karo*. *Third Circuit Opinion*, 620 F.3d at 312; *see also id.* at 320 (Tashima, J., concurring) (citing *Kyllo* for the proposition that government access to CSLI absent a showing of probable cause would violate the Fourth Amendment if that information "reveals a cell phone user's location within the interior or curtilage of his home"). Thus, the Fourth Amendment status

---

miles. MetroPCS Affidavit ¶ 4. But that does not indicate how precisely someone can be located. That depends not only on whether tower coverage is separated by sectors but also on the density of towers, and the affidavit is silent on whether its towers are sufficiently close together that some service areas overlap. Cell phone network coverage is rapidly becoming more dense, with the number of active cellular towers increasing by 11.5% each year. CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* at 9 (2009), *available at* http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf. As a result, cell site technology is increasingly accurate, *see Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones and Personal Locators*, 18 Harv. J.L. & Tech. 1, 311 n.12 (2004) ("[T]he more cell towers available . . . the more precisely one's movements can be tracked via cell transfers"). Furthermore, to extent that the affidavit indicates that some of its towers have ranges of only 100 yards, MetroPCS affidavit ¶ 4, this is certainly precise enough to pinpoint a phone's location within larger private properties not open to visual surveillance. Regardless, to the extent the court finds facts on precision necessary, and rejects those presented by Smith, the answer is to remand for an evidentiary hearing.

of CSLI at the very least poses a serious constitutional question warranting a discretionary denial of the government's application.

This conclusion is further bolstered by the D.C. Circuit's recent decision in the *Maynard* case, although as the magistrate judge notes, reliance on the *Maynard* precedent was not essential to his ruling but instead only provided additional support. *Smith Op.* at *8. In that case, the D.C. Circuit concluded that the government had violated the Fourth Amendment when it surreptitiously tracked a suspect's car using a GPS device for a period of 28 days, based on the holding that "[t]he whole of one's movements over the course of a month is not constructively exposed to the public" even if those movements are actually exposed to the public. *Maynard*, 615 F.3d at 561-62. As the Court persuasively explained, we maintain a reasonable expectation of privacy in our movements over time:

> A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain disconnected and anonymous…. In this way the extended recordation of a person's movements is . . . not what we expect anyone to do, and it reveals more than we expect anyone to know. . . .
>
> . . .
>
> . . . [P]rolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have . . . .

Id. at 563 (internal quotations and citations omitted). *Maynard*'s holding provided the magistrate judge with an additional basis to conclude that government access to 60 days worth of CSLI would violate the Fourth Amendment, by revealing the movements of the person carrying the phone over a prolonged period of time, and particularly considering that unlike the GPS device in *Maynard*, cell phones are routinely carried inside private spaces. *Smith Op.* at *8-10.

2. Cell Phone Providers' Ability to Access CSLI Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in CSLI.

The government contends that the magistrate judge erred in judging the question of reasonable expectation of privacy in CSLI based on the logic of *Karo* and *Maynard*, noting that neither case concerned business records held by a third party and arguing that a business'

customer can never have an expectation of privacy in such of records. Gov. Br. at 13-14. This argument, however, falls flat when matched against the Supreme Court's actual decisions concerning third party records. Moreover, the Third Circuit reached a directly contrary conclusion, holding that cell phone users may maintain a reasonable expectation in CSLI even though it is a record held by a third party business. *Third Circuit Opinion*, 620 F.3d at 317-18. In addition to being correct and persuasive authority, the *Third Circuit Opinion* also and at the very least demonstrates the existence of a serious constitutional question on this score, justifying exercise of the discretion granted under § 2703(d) to avoid the issue by requiring a warrant.

The government first missteps by fundamentally misreading the primary authority it cites for its argument, *United States v. Miller*, 425 U.S. 435 (1976), where the Supreme Court held that a bank depositer had no expectation of privacy in records about his transactions that were held by the bank. The government claims that this case stands for the proposition that a business' customer can never have an expectation of privacy in a third party business' records because they are not the customer's "private papers" but instead are "business records" belonging to the business, records in which a customer "can assert neither ownership nor possession." Gov. Br. at 13, quoting *Miller*, 425 U.S. at 440. However, that statement by the court was not the end of the analysis, and the Court proceeded to consider whether Miller nevertheless could maintain a reasonable expectation of privacy in the bank's records, noting that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442 (internal citation omitted). The conclusion of that analysis—that Miller had no such expectation—turned not on the fact that the records were owned or possessed by the banks, but on the fact that Miller "knowingly expose[d]" and "voluntarily conveyed" their contents to the bank. *Id.* (internal quotation marks and citation omitted); *see also Smith v. Maryland*, 442 U.S. 735, 744-45 (1979) (finding that telephone user did not possess an expectation of privacy in the telephone numbers he dialed because that information was "voluntarily conveyed" to the phone company).

Therefore, and contrary to the government's claim, there is no *per se* rule that a business' customer may never have an expectation of privacy in the contents of the business' records; rather, the question of expectation of privacy turns on whether the contents of those records were knowingly exposed and voluntarily conveyed to the business. And on that score, as the *Third Circuit Opinion* explicitly recognizes, CSLI is distinguishable from the bank records in *Miller* and the dialing information in *Smith*. *See Third Circuit Opinion*, 620 F.3d at 317-18. In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and knowingly conveyed to bank tellers and telephone operators or their automated equivalents. *See, e.g.*, *Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information . . . . The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."). Put simply, the phone customer knew what numbers he was exposing to the phone company; the bank customer knew what documents he was exposing to the bank.

The exposure of CSLI to a cell phone provider is nothing like the direct conveyance of phone numbers to an operator or bank documents to a teller. When a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed, and there is no indication to the user that making that call will also locate the caller, let alone generate a permanent record of this location; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all. *Third Circuit Opinion*, 620 F.3d at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."). Nor does this location information appear in the typical cell user's bill, a critical fact in *Smith*. *See Smith*, 442 U.S. at 742 ("All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."). In sum, the CSLI at issue is easily distinguishable from the information at issue in *Miller* and *Smith*. Consequently, *Karo* and *Kyllo* control the reasonable expectation of privacy analysis, not *Miller*

and *Smith*.

In its attempt to forestall this conclusion, the government claims—without any factual record to rely on—that all cell phone users realize that using a cell phone reveals their location to the cell phone provider, just like all telephone users (according to *Smith*) understand that dialing a telephone reveals that information to the phone company. Gov. Br. at 15, 17. Even if the government's sweeping claim were correct—and the Third Circuit's opinion amply demonstrates why the government is incorrect—that would not settle the question. Even the *Smith* Court recognized that the question of "knowing exposure" was not solely dispositive, or else *Smith* would have overruled the Court's previous holding that telephone callers maintain a reasonable expectation of privacy in their phone calls:

> A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."

Smith, 442 U.S. at 746-47 (Stewart, J. dissenting) (*quoting Katz v. United States*, 389 U.S. 347, 352 (1967)). Considering *Katz*, and rather than mechanically applying a "knowing exposure" rationale, the *Smith* Court also had to consider the *invasiveness* of the surveillance at issue, and relied on the conclusion that surveillance of dialed numbers was not meaningfully invasive of privacy:

> "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed-a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."

Smith, 442 U.S. at 741 (*quoting United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)). As already demonstrated above, CSLI is intensely revealing, exposing information about the interior of protected spaces and painting an intimate portrait of movements over an extended period of time that are reasonably expected to remain private, and therefore is distinguishable from the

telephone numbers in *Smith* on that basis as well.

Therefore and for example, even if T-Mobile users actually read and understand the privacy policy proffered by the government, Gov. Br. at 17-18, they may—and, in amici's view, do—still maintain an expectation of privacy in the location of their phones. Email users also understand that their email provider stores copies of their email content, and often may be subject to similar terms of service or privacy policies making clear that the provider may access that content in the ordinary course of business. Yet in a recent decision, the Sixth Circuit had no difficulty disagreeing with the government and concluding that email users maintain an expectation of privacy in their emails, even though the email provider's contract with the user made clear both the provider's ability and right to access those emails in certain circumstances. *See United States v. Warshak*, No. 08-3997, 2010 WL 5071766, at *12-13 (6th Cir. Dec. 14, 2010) (holding that the government needed to obtain a warrant and demonstrate probable cause to access email, despite terms of service that permitted the provider to access emails in some circumstances).

In conclusion, and particularly considering the recent *Third Circuit Opinion* and the decision in *Warshak*, the magistrate judge was correct to conclude that cell phone users maintain a reasonable expectation of privacy in their CSLI regardless of the purported third-party rule of *Smith* and *Miller*. To the extent this Court disagrees, however, and especially in light of the Supreme Court's caution in *Quon*, the appropriate course would be to uphold the denial of the government's application based on the discretion granted under § 2703(d), in order to avoid unnecessarily addressing this undeniably serious constitutional question.

3. The Fourth Amendment Requires the Government to Obtain a Search Warrant Based on Probable Cause Before Accessing CSLI.

Considering cell phone users' reasonable expectation of privacy in CSLI, the magistrate judge was correct to conclude that the government must obtain a search warrant based on probable cause before obtaining that data. The government takes issue with this conclusion, analogizing § 2703(d) orders to subpoenas and arguing that regardless of a cell phone user's

expectation of privacy, it need only satisfy a reasonableness standard to compel production of CSLI from a cell phone service provider regardless of the target's expectation of privacy. Gov. Br. at 21-25. Importantly, the government never made this argument to the magistrate judge, so his implicit disregard of it was not an abuse of his broad discretion under § 2703(d). Regardless, the government's simplistic analogy to traditional subpoenas is inapt for the simple reason that here, the person with a constitutional privacy interest in the records that the government seeks to obtain—the cell phone user—will not be notified of the compulsory process at issue, and therefore will have no opportunity to contest the order's reasonableness prior to the disclosure.[6]

The courts have consistently recognized that a warrant requires probable cause and a subpoena does not because a search and seizure conducted pursuant to a warrant is immediate and provides no opportunity for judicial review in advance, while a subpoena can be contested in court prior to enforcement. *See, e.g.*, *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (holding that while a subpoena can issue without a warrant, the subpoenaed party is protected because it can "question the reasonableness of the subpoena, before suffering any penalties for refusing to comply with it, by raising objections in an action in district court" (internal citations omitted)); *Zurcher v. Stanford Daily*, 436 U.S. 547, 561 (1978) (assuming that "the subpoena *duces tecum* offer[s] . . . the opportunity to litigate its validity" before compliance); *See v. City of Seattle*, 387 U.S. 541, 544-45 (1967) ("[T]he subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply."); *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 195 (1946) (noting that subpoenas become enforceable only "after adequate opportunity to present objections"); *id*. at 217 ("To [the subpoena] they may make 'appropriate defense' surrounded by every safeguard of judicial restraint."); *In re Doe*, 253 F.3d 256, 264 (6th Cir. 2001) (holding that one "primary reason" warrants require probable cause and subpoenas require only reasonableness is that "unlike 'the immediacy and

[6] The Stored Communications Act only requires prior notice to a customer when the government seeks the content of communications without a warrant, *see* 18 U.S.C. § 2703(b), and even that notice may be delayed by obtaining a court order under the liberal standards of 18 U.S.C. § 2705.

intrusiveness of a search and seizure conducted pursuant to a warrant,' the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced" (citation omitted)); *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000) (emphasizing that subpoenas do not require probable cause precisely because they "commence[] an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process" (internal citations omitted)); *see also In re Nwamu*, 421 F. Supp. 1361, 1365 (S.D.N.Y. 1976) (holding that government agents' seizure of corporation's items over employees' objections, pursuant to a "forthwith" subpoena duces tecum, was an unlawful seizure in violation of the Fourth Amendment, because corporation was denied opportunity "to raise and litigate" the issue of probable cause "before the judge attending the grand jury proceedings").

Where—as here—the government secretly seeks to compel disclosure through a third party of information in which the target possesses a Fourth Amendment-protected reasonable expectation of privacy, it short-circuits this process, preventing the target from contesting the reasonableness of the government's demand. As in *In re Nwamu*, "[t]he very existence of a right to challenge [a compelled disclosure] presupposes an opportunity to make it. That opportunity [will be] circumvented, frustrated and effectively foreclosed by the methods employed here." *Id*. Such an invasion of an expectation of privacy, without any opportunity for the holder of that expectation to challenge the invasion, is indistinguishable from—indeed, is—a search requiring a probable cause warrant.

The reasoning of modern Supreme Court decisions concerning third party subpoenas—in particular, *Miller* and *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984)—supports rather than undermines the conclusion that compelled disclosure violates the Fourth Amendment where the subject of the information sought possesses a reasonable expectation of privacy in that information but is given no opportunity to challenge the disclosure. In former case, it was only *after* concluding that defendant Miller had no privacy expectation in the bank records at issue

that the Court concluded that the traditional subpoena rules would apply, and that because the recipient bank had not challenged the subpoena's validity on reasonableness grounds, it did not need to evaluate whether they were reasonable. *Miller*, 425 U.S. at 442-46; *see also id.* at 444 ("*Since no Fourth Amendment interests of the depositor are implicated here*, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant[.]" (emphasis added)). Therefore, *Miller* does not directly speak to or establish what standards would apply to a third party subpoena for materials in which an un-notified target maintains an expectation of privacy,[7] which is made all the clearer when examining the latter case, *SEC v. O'Brien*.

In *O'Brien*, targets of an SEC investigation sought injunctive relief to require prior notice of SEC subpoenas to third parties so that they could assert their Fourth Amendment rights. 467 U.S. at 739. Only after concluding that the targets lacked a reasonable expectation of privacy in bank records subpoenaed by the SEC did the Supreme Court conclude that the targets were "disable[d] . . . from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers." *Id.* at 743. The necessary implication of this ruling is that such an argument does exist and was not rejected by the Supreme Court. Otherwise, an analysis of whether the targets possessed a reasonable expectation of privacy in the records would have been unnecessary. The Supreme Court did not rule on that argument, and therefore did not rule it out.

Consequently, several state courts considering their own state constitutions have

[7] The Supreme Court's analytical approach in *Miller* stands in sharp contrast to the one case that the government can directly cite for the proposition that third party subpoenas are judged on reasonableness regardless of the target's expectation of privacy in those records, *United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976). *Palmer*, which was decided within six weeks of *Miller* and did not cite that case at all, failed to consider the reasonable expectation of privacy question that the *Miller* Court found to be so central to the issue and instead simply assumed that even if there were an expectation of privacy, "a properly limited subpoena does not constitute an unreasonable search and seizure under the fourth amendment." *Id*. at 1282. Considering its disregard of and inconsistency with the logic of *Miller*, this case is simply not persuasive authority.

concluded that notice to the target is required where subpoenas seek third party records in which the target possesses a reasonable expectation of privacy, recognizing that government access to such records without an opportunity to challenge the subpoena would amount to a search or seizure. For example, the Colorado Supreme Court, when considering subpoenas for bank records—in which the customer possesses a reasonable expectation of privacy under the Colorado Constitution if not under *Miller*—has concluded that prior notice to the customer is necessary to avoid unreasonable search and seizure. See *People v. Lamb*, 732 P.2d 1216, 1220-21 (Colo. 1987); *see also, e.g.*, *King v. State*, 535 S.E.2d 492, 495-96 (Ga. 2000). As the *Lamb* court held:

> [U]nder the Colorado Constitution a bank customer has a reasonable expectation of privacy in the bank's records of the customer's financial transactions. As a result, those records are protected by the Colorado Constitution against unreasonable searches and seizures. The core value to which constitutional protection is extended is the customer's privacy interest. In order to give effect to that protection, the customer must have an opportunity to test the constitutional validity of an administrative subpoena before it is executed. The availability of a hearing subsequent to production and disclosure of bank records is inadequate because once the privacy interest has been violated there is no effective way to restore it.

732 P.2d at 1220.

The same reasoning applies here, where the cell phone user has a Fourth Amendment-protected reasonable expectation of privacy in the CSLI that is sought by the government. Hence, the *Third Circuit Opinion* assumed that the Fourth Amendment would require probable cause to the extent that CSLI sought with a § 2703(d) order would reveal information about the interior of a home that is protected under *Karo*. *Third Circuit Opinion*, 620 F.3d at 312-313; *see also id.* at 320 (Tashima, J., concurring). Even more recently, the Sixth Circuit in the *Warshak* case had no difficulty in holding that a §2703(d) order to an email provider to obtain emails in which the customer maintained a reasonable expectation of privacy would violate the Fourth Amendment, despite the government pressing the same "reasonableness" argument that it does here. Supplemental Response of the United States to Section II of Defendants' Omnibus Pretrial Motions at 4-9, *United States v. Warshak*, No. 08-3997, 2010 WL 5071766 (6th Cir. Dec. 14,

2010). After deciding that email users possess a reasonable expectation of privacy in the emails they store with third party email providers, the *Warshak* court concluded that "it is manifest that agents of the government cannot compel a commercial ISP [or "Internet Service Provider"] to turn over the contents of an email without triggering the Fourth Amendment," and "[i]t only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception." 2010 WL 5071766 at *12.

Particularly considering such precedent, the magistrate judge reached the same—and in amici's view, correct—conclusion: the compelled disclosure of third party materials in which a target maintains a reasonable expectation of privacy, without the target receiving any notice or opportunity to challenge the government's demand, is a Fourth Amendment search requiring probable cause. Indeed, because the Supreme Court has yet to directly address this argument, there obviously remains a serious constitutional question justifying the exercise of a court's discretion under § 2703(d) to deny the government's application and thereby avoid the issue.

CONCLUSION

For the foregoing reasons, the decision of the magistrate judge should be affirmed. However, if the Court concludes that more factual development is necessary, it should remand to the magistrate judge for that purpose.

Dated: January 14, 2011

Respectfully submitted,

Kevin S. Bankston
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
Tel: (415) 436-9333 x126
Fax: (415) 436-9993

Catherine Crump
Benjamin T. Siracusa Hillman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 519-7806
Fax: (212) 549-2651

/s/ *Lisa Graybill*
Lisa Graybill
Attorney-in-Charge
Legal Director
Texas Bar No. 24054454
Southern District Bar No. 784838
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF TEXAS
P.O. Box 12905
Austin, TX 78711
Tel: (512) 478-7300 ext. 116
Fax: (512) 478-7303

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 14th day of January, 2011, the attached **BRIEF IN OPPOSITION TO THE GOVERNMENT'S REQUEST FOR REVIEW** was filed electronically through the CM/ECF system. Service has been automatically accomplished through the Notice of Electronic Filing.

/s/ Lisa Graybill
Lisa Graybill